140 سلسلة محاضرات الإمارات

حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية

ريتشارد كلارك وروبرت نيك



مركز الإمارات للدراسات والبحوث الاستراتيجية

بسم الله الرحمن الرحيم

تأسس مركز الإمارات للدراسات والبحوث الاستراتيجية في 14 آذار/ مارس 1994، بوصفه مؤسسة مستقلة تهتم بالبحوث والدراسات العلمية للقضايا السياسية والاقتصادية والاجتماعية، المتعلقة بدولة الإمارات العربية المتحدة ومنطقة الخليج العربي على وجه التحديد، والعالم العربي والقضايا الدولية المعاصرة عموماً.

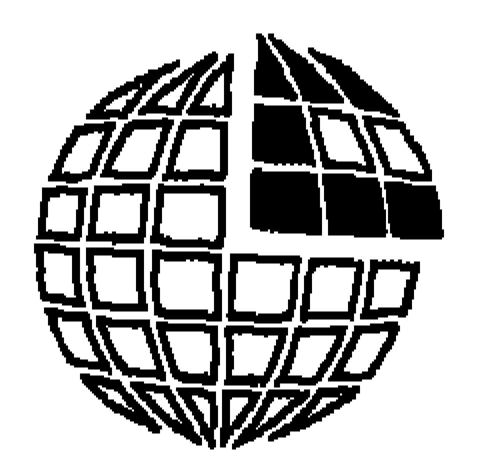
من هذا المنطلق يقوم المركز بإصدار «**سلسلة محاضرات الإمارات**» التي تتناول المحاضرات، والندوات، وورش العمل المتخصصة التي يعقدها المركز ضمن سلسلة الفعاليات العلمية التي ينظمها على مدار العام، ويدعو إليها كبار الباحثين والأكاديميين والخبراء؛ بهدف الاستفادة من خبراتهم، والاطلاع على تحليلاتهم الموضوعية المتضمنة دراسة قضايا الساعة ومعالجتها. وتهدف هذه السلسلة إلى تعميم الفائدة، وإغناء الحوار البنّاء والبحث الجاد، والارتقاء بالقارئ المهتم أينما كان.

سلسلة محاضرات الإمارات

- 140 -

حماية الفضاء الإلكتروني
في دول مجلس التعاون لدول الخليج العربية

ريتشارد كلارك وروبرت نيك



تصدر عن

مركز الإمارات للدراسات والبحوث الاستراتيجية

محتوىٰ المحاضرة لا يعبِّر بالضرورة عن وجهة نظر المركز

ألقيت هذه المحاضرة يوم الثلاثاء الموافق 18 أيار/ مايو 2010

الطبعة الأولى 2011

ISSN 1682-122X

النسخــة العاديـــة ISBN 978-9948-14-390-1

النسخة الإلكترونية ISBN 978-9948-14-391-8

توجه جميع المراسلات إلى رئيس التحرير على العنوان التالي:

سلسلة محاضرات الإمارات ـ مركز الإمارات للدراسات والبحوث الاستراتيجية

ص. ب: 4567

أبوظبي ـ دولة الإمارات العربية المتحدة

هاتف: 4044541-9712+

فاكس: 4044542-9712+

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

مقدمة

أصبح الفضاء الإلكتروني مكاناً خطراً بالنسبة للبلدان الصغيرة، فخلال السنتين الماضيتين قام معتدون غرباء بحرمان ما لا يقل عن ثلاث دول من استخدام هذا الفضاء. لقد اجتاح مجرمو الفضاء الإلكتروني عدداً من البلدان في أوربا الشرقية والكاريبي، وتقدَّر اليوم العوائد غير المشروعة من الجريمة الإلكترونية بما يزيد على 1 ترليون دولار أمريكي حول العالم. وتقوم الشركات باستخدام شبكة الإنترنت لممارسة التجسس الصناعي وسرقة استراتيجيات التفاوض الخاصة بالحكومات والمنافسين وسرقة المعادلات الصناعية ومخططات المصانع ورموز الحواسيب.

وفي الوقت ذاته تزداد الدول شراهة في استخدام الفضاء الإلكتروني، حيث انخرطت في عمليات تجسس على مستويات لم يسبق لها مثيل، وأعدّت ساحات المعركة لحروب لم يخطر ببال أحد أنها ستقوم. وتشهد هذه التوجهات تسارعاً محموماً لتشكل مجتمعة تهديداً يؤدي إلى تقويض الثقة بشبكة الإنترنت وتهميش مزايا الكفاءة الناتجة عن استخدام الأنظمة المتصلة بالإنترنت، ما قد يؤدي نهاية المطاف إلى زعزعة الشبكة العالمية التشاركية الوحيدة التي بتنا جميعاً نعتمد عليها.

وفي حين تصارع الولايات المتحدة الأمريكية والاتحاد الأوربي والدول الأخرى من دون انقطاع للتوصل إلى كيفية حل هذه المشكلات، تتمتع دول

مجلس التعاون لدول الخليج العربية بفرصة لتظهر سبّاقة في هذا المجال. ففي هذا العقد سيكون للأمن الإلكتروني كلمة الفصل في السوق، ولا يقتصر ذلك على المنتجات والشركات بل يمتد ليشمل الدول والأقاليم. وبالطبع عند اتخاذ الشركات قراراتها حول أماكن إنشاء مراكز بياناتها الجديدة ومرافق إنتاجها، فإنها ستختار البلدان التي لديها تشريعات قانونية تنص على معاقبة مجرمي الفضاء الإلكتروني، بما يضمن حماية خصوصية المستخدمين وصون حقوق الملكية الفكرية. وتريد الشركات أن تطمئنّ إلى وجود أجهزة تحريات وسلطات قضائية لدعم التشريعات القانونية، كما تريد وضع أنظمتها على شبكات محلية لم يُصبها وباء الفيروسات، ولا تتهددها شبكات "البوت نت"* (Botnets). وسترغب الشركات أيضاً في معرفة أن هذه البلدان قادرة على حماية نفسها في مجال الإنترنت وضمان توفير مستويات عالية من التواصل العالمي.

وتشير أربعة عوامل رئيسية إلى أن بإمكان دول مجلس التعاون لدول الخليج العربية أن تصبح "منطقة إلكترونية آمنة"، ما يشجّع الشركات على إقامة أعمالها في دول المجلس. أول هذه العوامل التعداد السكاني القليل وبالتالي قلة إجمالي عدد مستخدمي الإنترنت وصغر حجم الشبكة. والثاني

* هي شبكة تتكون من مجموعة من الحواسيب يسيطر عليها مخالفو القانون وموجهو الجريمة على شبكة الإنترنت من خلال "البوت"، وهي برامج إلكترونية خبيثة يتم تنزيلها على الأجهزة المصابة من دون ملاحظة أصحاب الأجهزة المصابة، وتدار عن بعد بوساطة خادم التحكم (C2S)، ويصعب أحياناً اكتشافها بالبرامج المضادة للفيروسات. (المحرر)

يتمثل في كون دول الخليج غنية نسبياً بما يتيح الاستثمار في مجال الأمن الإلكتروني بما يحقق عوائد مؤكدة. والثالث أن الحكومات تمتلك جميع المؤسسات التي تقدم خدمة الإنترنت (ISP) بما يسمح لدول الخليج بتطبيق متطلبات أمنية جديدة بسهولة. والرابع أن استخدام تقنيات الإنترنت في دول الخليج يعد أمراً حديثاً نسبياً، وبالتالي فإن الأفراد ليسوا غارقين في أسطورة أن الإنترنت هو أمر خارج عن سيادة الدولة، وأن الحكومات غير مضطرة إلى تحقيق الأمن في هذا المجال.

ينظر هذا البحث في مكونات الفضاء الإلكتروني الآمن، ويبدأ بتقويم المخاطر المحيطة بالفضاء الإلكتروني في دول الخليج، بما في ذلك تقويم التهديدات التي تشكلها قدرات حرب الفضاء الإلكتروني لدى الأطراف الإقليمية، ونقاط الضعف التي قد تستغلها هذه الأطراف. كما يناقش البحث العواقب المحتملة في حال تمكنت هذه الأطراف من استهداف نقاط الضعف في دول مجلس التعاون لدول الخليج العربية. ويضع البحث خريطة طريق يمكن أن تؤدي إلى تحويل منطقة الخليج العربي إلى فضاء إلكتروني آمن.

المخاطر الإقليمية

إذا أردنا تعريف المخاطر فيمكننا القول إنها نتاج لاجتماع التهديدات ونقاط الضعف والعواقب. وباستخدام هذا الوصف يُعاين هذا البحث التهديدات الإلكترونية التي تتعرض لها دول مجلس التعاون لدول الخليج العربية من قبل الأطراف الإقليمية، ونقاط الضعف التي قد تستغلها هذه

الأطراف، والعواقب التي قد تنشأ في حال تمكنت الأطراف من استغلال نقاط الضعف هذه. ويمهد البحث الطريق لوضع خطة من أجل تأمين الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية.

التهديدات

على رغم أن الإنترنت تفتح المجال للهجمات من أي مكان حول العالم، فإن الهجمات التي تستهدف دول مجلس التعاون لدول الخليج العربية غالباً ما تأتي من الدول المجاورة في المنطقة أو من أطراف غير حكومية يرتبط نشاطها بالتوترات والمظالم الإقليمية. وكما هي الحال في أمريكا الشمالية وأوربا وآسيا فإن في الشرق الأوسط عدداً لا يُستهان به من المنظمات القادرة على القيام بعمليات تخريبية في فضائه الإلكتروني. وتشير التقارير إلى أن كلاً من سورية وتركيا وإسرائيل قد استثمرت أموالاً طائلة لتطوير إمكاناتها لشنّ هجمات إلكترونية. وعلى رغم قلة المعلومات حول هذه البرامج، فإن برنامج إيران الخاص بحرب الفضاء الإلكتروني قد حظي باهتمام خاص. وفي ظل المعلومات المتوافرة بصورة عامة، فقد ركز هذا البحث على أنشطة إيران الإلكترونية.

أشار البرنامج الإخباري "فرونتلاين" *Frontline* الذي تبثّه قناة "بي بي أس" PBS الأمريكية إلى أن الحرس الثوري الإيراني قد أسس عام 2005 شعبة متخصصة في حرب الفضاء الإلكتروني، وقد استقطب قوتها العاملة من ثلاث مجموعات قرصنة في إيران، وهي: "أشيانة" و"شابجارد"

و"سيمورغ". كما يعتمد هذا الجيش الإلكتروني على مهارات خارجية، وقد أسس شركات خاصة للتوظيف والتدريب واستخدام التقانة.[1]

وفي أيار/ مايو 2010 صرّح مسؤول كبير في الحرس الثوري الإيراني بأن «الجيش الإلكتروني التابع للحرس الثوري قد استطاع اليوم أن يصبح ثاني أقوى جيش إلكتروني في العالم».[2] وعلى رغم عدم وضوح أسس هذا الادعاء، تعتقد شركة الأبحاث الأمريكية "ديفنس تك" أن الشعبة الإلكترونية لديها حوالي 2400 موظف بالإضافة إلى 1200 من قراصنة الإنترنت (الهاكرز) في القطاع الخاص، ويُعتقد أن ميزانيتها السنوية تفوق 75 مليون دولار.[3] وحتى الآن اقتصرت أنشطة إيران في حرب الفضاء الإلكتروني على هجمات ضد مواقع إلكترونية، كتخريب أو حجب مواقع لشركات إخبارية تغطي حركات المعارضة الإيرانية. وفي 19 كانون الأول/ ديسمبر 2009 تعرَّض موقع "تويتر" للمدوّنات لهجمات تسببت بإغلاقه في عدة مناطق من العالم. وقد أعيد توجيه المستخدمين الذين حاولوا دخول هذا الموقع إلى رسالة تقول:

> «تعتقد الولايات المتحدة الأمريكية أنها تتحكم بشبكة الإنترنت وتسيطر عليها، لكنها مخطئة، فنحن بقوتنا نتحكم بالشبكة، لذا لا تحاولوا استفزاز الشعب الإيراني... من منا على قائمة الحظر الآن، إيران أم الولايات المتحدة الأمريكية؟ إننا نضعهم على قائمة الحظر، فاحذروا».[4]

وبعد شهر من هذه الحادثة تعرض محرك البحث الصيني "بايدو" إلى هجوم مشابه، حيث تم تشويه الصفحة الرئيسية للموقع بعبارة مفادها: «تم

تأسيس جيش إيران الإلكتروني للاعتراض على تـدخلات المواقـع الأجنبيـة والصهيونية في الشؤون الداخلية لدولتنا ونشر الأخبار الكاذبـة والمـضلّلة».[5] ومن غير الواضح سبب تعرُّض موقع صيني لهجوم مـن هـذا النـوع، إلا أن الرد جاء سريعاً من قراصنة الشبكة في الصين، حيـث وجَّـه الاتحـاد الـصيني للقرصنة الإلكترونية، وهو جماعة استهدفت مراراً مواقع أمريكية في السابق، ضربة انتقامية ضد سلسلة من المواقـع الإلكترونيـة الإيرانيـة التـي اختـيرت بشكل عشوائي في هجمات مشابهة، وبثّت الجماعة رسائل على هذه المواقع رداً على تلك المنشورة على موقع "بايدو".[6]

إن تشويه المواقع الإلكترونية أسلوب يتبعه الهواة، وهو أقرب ما يكون إلى التخريب والعبث الصبياني منه إلى الحـرب. ومـن الخطـأ اعتقـاد أن هـذه الأنماط من الهجمات تعكس القدرات الكاملة التي يتمتع بها النظام الإيـراني. ويتضح من التصريحات العلنية أن إيران تدرك أنها موضع استهداف هجمات أكثر تعقيداً، وبالتالي فإنها تعمل على تطوير إمكانات بمقـدورها مجاراة هـذه التهديدات. وقد علّق مؤخراً وزير الدفاع الإيراني أحمد فهيـدي علانيـة عـلى اسـتعدادات إيـران لخـوض حـرب فـضاء إلكـتروني قـائلاً: «تعـد تقنيـات المعلومـات والاتـصالات حاليـاً في غايـة الأهميـة لمختلـف الـدول وعلينـا الاستعداد وتجهيز أنفسنا ضد كافة أشكال الحرب الإلكترونية».[7]

وتضع "ديفنس تك" إيران ضمن قائمة أقوى خمس دول في العالم مـن حيث قدراتها الهجومية الإلكترونية، كما تبيّن لائحـة بـأنواع أسـلحة الفـضاء الإلكــتروني التــي تــشكل ترســانة إيــران، وتتــضمن أســلحة النــبض

الإلكترومغناطيسي، وأدوات تشويش البيانات اللاسلكية، وأحصنة طروادة الخفية، والفيروسات، والديدان الإلكترونية.

في تموز/ يوليو 2009 صرّح خبير الدفاع الإسرائيلي، ألون بن ديفيد لقناة "إيه بي سي" ABC الإخبارية أن إسرائيل دأبت من خلال حملة شنتها على الشبكات العسكرية الإيرانية على تخريب أو إتلاف معلومات تتعلق ببرنامج إيران النووي البحثي.[8] كما أفادت تقارير إيه بي سي أن إسرائيل والولايات المتحدة الأمريكية قد بدأتا برنامجاً لتخريب برمجيات وأجهزة اشترتها إيران من الخارج لاستخدامها في البحث النووي.[9] وصرّح مسؤولون إيرانيون مؤخراً أنه قد تم تدمير شبكة من أجهزة التنصت المزروعة في الفضاء الإلكتروني الإيراني بغرض جمع المعلومات حول برنامجها النووي.[10] وفي ظل ازدياد التوتر بين إيران وإسرائيل، من المرجح تصعيد أنشطة الهجمات الإلكترونية بينهما.

ونظراً لحقيقة أن ما يزيد على مئة دولة قد طوَّرت أو تعمل على تطوير قدراتها الهجومية الإلكترونية، فمن المتوقع أن تشكل حرب الفضاء الإلكتروني جزءاً هاماً من كافة الصراعات المستقبلية، كما ستلعب الأسلحة الإلكترونية الافتراضية دوراً قد يكون حاسماً في الحرب الفعلية. وستكون الغلبة للدولة التي تتفوق في حماية فضائها الإلكتروني وتعطيل فضاء أعدائها بعد أن تضمن قدرة جيشها على استخدام تقنية المعلومات وشن هجمات في الفضاء الإلكتروني الافتراضي بما يُحدِث آثاراً ملموسة. وفي هذا الصدد تتمتع الحرب الإلكترونية بقدرة تغيير موازين القوى في الصراعات التقليدية، إلا

أن خطراً أكبر قد يكمن في استخدام الهجمات الإلكترونية لأغراض إجرامية. وعلى رغم قوة إجراءات تطبيق القانون في دول الخليج، فإن ذلك لم يحل دون تعرضها لمشكلة الجريمة الإلكترونية.

أشارت مؤسسة "تريندمايكرو" TrendMicro المتخصصة بالأمن أنه خلال عام 2009 تسبب قراصنة الإنترنت بتعطيل حوالي 800 ألف نظام في المملكة العربية السعودية، وأن الدافع وراء معظم هذه الهجمات كان دافعاً مالياً. وفي دولة الإمارات العربية المتحدة تسبب قراصنة الإنترنت بتعطيل حوالي 250 ألف نظام، وفي كلا البلدين تم تعقُّب هذه الهجمات ليتبين أن معظمها قادم من مواقع خارج نطاق الدول المستهدَفة.[11] وفي عام 2008 وقَعت وزارة التربية والتعليم ووزارة العمل في دولة الإمارات العربية المتحدة ضحية لهجمات تصيُّد كان الهدف منها جمع معلومات شخصية من زوار الموقع، حيث أنشأ متسللو الإنترنت المسؤولون عن هذه الحادثة مواقع مطابقة تقريباً للموقع الرسمي www.moe.gov.ae والموقع www.mol.gov.ae تحت اسم www.mol.gov.tk وwww.moe.gov.tk وهي مواقع مسجلة في إقليم "توكيلاو" في نيوزيلندا.[12]

وفي آذار/ مارس 2010 حذّرت شرطة أبوظبي من ازدياد أنشطة الجرائم الإلكترونية التي تستهدف الأفراد للحصول على معلومات حول حساباتهم المصرفية.[13] قد تكلف الجريمة الإلكترونية الأفراد المقيمين في دول الخليج والشركات العاملة فيها المليارات، الأمر الذي من شأنه أن يقلل من جاذبية المنطقة بالنسبة للمستثمرين الأجانب والمقيمين المحتملين. لذا يجب

اتخاذ خطوات موازية لتهديدات الدول لتخفيف تهديدات أنشطة الجريمة الإلكترونية وسد الثغرات أمامها والحد من نتائجها.

نقاط الضعف

هناك عدد هائل من نقاط الضعف في معظم الشبكات المحلية ما يجعل البلدان عرضة لهجمات إلكترونية. وأكثر نقاط الضعف هذه تعد متأصلة في البنية الهندسية للشبكات والبروتوكولات التي تنظم التواصل فيما بينها. وهذا البحث يركز على نقاط الضعف العامة أمام هجمات الحرمان من الخدمة (DDOS) والهجمات على البنية التحتية، والهجمات على الشبكات الحكومية والعسكرية.

هجمات الحرمان من الخدمة

استخدمت روسيا في ثلاث مناسبات مختلفة هجمات الحرمان من الخدمة ضد دول كانت تابعة لها في السابق في أوربا الشرقية وآسيا الوسطى. ففي عام 2007 تعرضت إستونيا لهجمات الحرمان من الخدمة بعد أن أزالت تمثالاً لجندي في الجيش السوفيتي من ساحتها المركزية، وهو نصب تذكاري شيّده الروس خلال مدة احتلالهم للبلد بعد الحرب العالمية الثانية. وفي تلك الحادثة قام قراصنة الإنترنت الروس "الوطنيون" بإغراق الفضاء الإلكتروني للبلد بسيل من ملايين الأوامر والطلبات لصفحات إلكترونية. ولم تقتصر الهجمات على المواقع الإلكترونية، بل استهدفت عناوين بروتوكول الإنترنت الخاصة بالأنظمة الهاتفية والمصرفية.

وبعد سنة ونصف السنة عندما اندلعت أعمال العنف بين روسيا وجمهورية جورجيا، تم استدعاء شعبة الهاكرز الروس للخدمة مجدداً. وقد تزامنت الهجمات الإلكترونية هذه المرة مع الهجمات الفعلية الأرضية والجوية. واستخدم الروس شبكات "البوت" لإطاحة الحكومة الجورجية والمواقع الإلكترونية الإعلامية، وإغراق المجال الإلكتروني للبلاد بزحام خانق بحيث يتعذّر على الحزم الإلكترونية الأخرى دخول البلاد أو الخروج منها. كما سيطر القراصنة على مُوجِّهات الاستقبال للتأكد من التحكم بأي حركة مرور قد تتسرب. وبعد ستة أشهر لجأ الروس إلى هذا الأسلوب مرة أخرى، وكان الهدف هذه المرة جمهورية قرغيزستان في آسيا الوسطى، حيث تم تعطيل الإنترنت في البلد لأكثر من أسبوع.

الهجمات على العمليات الحكومية والعسكرية

تتعرض الأنظمة الحكومية والعسكرية لهجمات يومية في جزء من عمليات التجسس، وتمارس عدة دول هذه العمليات التي تهدف إلى سرقة تصاميم أنظمة الأسلحة أو الحصول على المعلومات المفيدة بسرقة مخططات المعارك، أو فهم طرق تفكير الأعداء المحتملين، أو الإعداد لتعطيل الشبكات وحرمان جيوش العدو من استخدامها في أثناء الحرب. ويعد أي نظام متصل بالإنترنت عرضة للهجوم، كما يعد أي نظام متصل بنظام متصل بالإنترنت عرضة للهجوم أيضاً. لذا قد تجد الحكومات والجيوش التي تعتمد في القيام بوظائفها الرئيسية على هذه الأنظمة أنها غير متوافرة أو لا يمكن الاعتماد عليها عندما تكون في أمسّ الحاجة إليها. وبالتالي فإن ميزة الشبكة العسكرية

المتفوقة التي يتمتع بها جيش يتسلح بالتقانة الحديثة قد تذوي وتزول تماماً بفعل الهجمات الإلكترونية.

الهجمات على البنية التحتية الحساسة

مع أن آثار هجمات الحرمان من الخدمة قد تبدو ضئيلة نسبياً من الناحية التقانية فإنها قد تكون مدمرة على الصعيد الوطني، ولا يجوز إطلاقاً الاستهانة بالخسائر الاقتصادية المحتملة التي قد يتكبدها البلد خلال أسبوع من الشلل الذي قد يصيبه جراء انقطاع خدمات الإنترنت عنه. وفي البلدان التي تتمتع بأنظمة عسكرية متطورة تعتمد على تقنيات الشبكة، بإمكان هذه الهجمات أن تقلل من جهوزية تلك الأنظمة وفاعليتها، وغالباً ما تقتصر آثار هذه الهجمات على الفضاء الإلكتروني، إلا أنه في ظل تزايد استخدام أنظمة التحكم الصناعي للإنترنت من أجل تشخيص الأنظمة وإعادة ضبطها وتنفيذ الوظائف الإدارية الأخرى، أصبح بإمكان العابثين والأوغاد الإلكترونيين السيطرة والتحكم عن بعد بوظائف أنابيب الغاز ومرافق إنتاج الوقود والمصانع الكيماوية والمحطات الكهربائية. وفي أي من هذه الحالات قد ينتج عن التلاعب بالبرمجيات المتحكمة في هذه الأنظمة ضرر وإرباك حقيقي على مستوى العالم.

وقد أجرى مختبر أيداهو الوطني التابع للحكومة الأمريكية عام 2006 تجربة أظهرت كيفية تدمير مُولِّد في شركة خدمات عن طريق شن هجوم عبر الإنترنت. وقد تم توصيل المولِّد إلى نظام مخبري بطريقة تحاكي الأسلوب

الواقعي المتبع لدى شركات الكهرباء في توصيل الأنظمة، ثم تم الدخول عن بعد إلى نظام المولِّد وإعطاؤه أوامر أحدثت فيه فرقعة وارتجاجاً ثم انفجر من تلقاء نفسه. والجدير بالذكر أن هذه المولِّدات تحتاج ستة أشهر لتصنيعها ويتم إنتاجها حسب الحاجة فقط.

النتائج

إن نتائج أي من هذه الهجمات أمر بديهي، فنظراً لاعتمادنا على التقنيات المتصلة بشبكة الإنترنت بإمكان هجوم الحرمان من الخدمة الذي يستهدف شبكة وطنية أن يصيب بلداً كاملاً بحالة شلل كلية خلال أيام، إلا أن انعكاسات هذا الهجوم قد تدوم لمدة أطول. وفي العقد القادم سيشكل الفضاء الإلكتروني الميدان الذي تبني فيه الدول سمعتها أو تخسرها. فالبلدان التي لا تستطيع ضمان استخدام الإنترنت بشكل مستمر، لن تشكّل أماكن جذب للاستثمار أو العمل أو العيش فيها.

يعتمد اقتصاد منطقة الخليج العربي بشكل أساسي على استخراج ومعالجة النفط والغاز، كما أن مولدات الكهرباء التي تعتمد عادة على النفط والغاز وقوداً تعد ضرورية لاستمرار استخراج ومعالجة الهيدروكربونات. وبما أن هذه المنطقة تعتمد بشكل كبير على أنظمة التبريد خلال أشهر الصيف الحارة، فإذا تعطلت مولدات الكهرباء هنا فإن قدرة السكان على الاستمرار ستكون موضع تهديد. كما أن محطات تحلية المياه تعتمد على البنية التحتية المولدة للكهرباء وغالباً ما تبنى بجانبها. فإذا ما تعرضت أي من هذه البنى

التحتية لهجوم إلكتروني يعطلها فإن النتائج ستكون مدمرة. وأخيراً يمكن القول إن باستطاعة الهجمات الإلكترونية ضد الأنظمة الحكومية والعسكرية أن تقوض قدرة الحكومة في الحفاظ على النظام وتقديم الخدمات المدنية والعسكرية للدفاع عن الحدود الوطنية وإظهار قوتها في الخارج، وستكون التكاليف باهظة في حال عدم معالجة مواضع الضعف هذه.

خطة العمل

مع استمرار ربط العمليات الحيوية بالإنترنت واشتداد شراسة الأنشطة الخبيثة على الشبكات، فإن سلامة الفضاء الإلكتروني للدول ستشكل عنصراً جوهرياً في قرارات الشركات حول أماكن إنشاء أعمالها. وبالتالي فإن الأمن الذي كان يعد مجرد تكلفة يجب تخفيضها سيصبح صاحب الكلمة في السوق. فالبلدان التي لم تحصِّن شبكاتها الوطنية من شأنها أن تجتذب المجرمين والمتسللين الإلكترونيين وتحرضهم على ممارسة اعتداءاتهم، ولا يقتصر الأمر على ذلك بل ينال النمو الاقتصادي للبلاد فيعوقه. ولهذه الأسباب يجب على دول مجلس التعاون اتخاذ خطوات لتحويل منطقة دول المجلس إلى "منطقة فضاء إلكتروني آمن وسليم". وكانت الاستراتيجية الوطنية لأمن الفضاء الإلكتروني في الولايات المتحدة لعام 2003 قد اقترحت أمريكا الشمالية لهذا الدور، ولكن هذه الفكرة لم تدخل حيز التنفيذ إطلاقاً. وتعد الإجراءات التالية من أهم العناصر المكونة لمنطقة إلكترونية آمنة:

- تحسين أمن نظام أسماء النطاقات (DNS) في دول مجلس التعاون؛

- التركيز على سلامة الشبكة الوطنية؛
- توطيد التعاون لمعالجة الجرائم الإلكترونية؛
- إعداد خطط تعاونية لتخفيف آثار هجمات الحرمان من الخدمة؛
- تعزيز البنية التحتية الحساسة؛
- حماية الأنظمة الحكومية والعسكرية وتحصينها.

تحسين أمن نظام أسماء النطاقات (DNS) في دول مجلس التعاون لدول الخليج العربية

إن نظام أسماء النطاقات هو عبارة عن دليل هاتف للإنترنت، فهو يُتيح لمشغِّل الحاسوب طباعة عنوان سهل التذكُّر مثل www.google.com للدخول إلى هذا الموقع بدلاً من أن يضطر إلى تذكُّر 72.14.204.99. ومثل بقية البروتوكولات الأساسية التي تجعل الإنترنت تعمل، لم يتم تصميم نظام أسماء النطاقات ليكون آمناً. إذ يمكن بسهولة تقليد النظام فيتمكن المهاجم الذي يشن هجومه من السيطرة على النطاق والقيام بالاحتيال أو أي نشاط خبيث آخر. وقد تم استغلال نقطة الضعف هذه في الهجوم الإيراني على موقع بايدو الصيني الذي ذكرناه سابقاً.

وتقوم منظمات الجريمة بشراء مواقع إلكترونية في جزء من عمليات الاحتيال باستخدام الشبكة بالإضافة إلى هجمات التصيد أو الأعمال الخيرية

المزيفة أو عروض الخدمات الكاذبة، كما يستخدَم النظام للسيطرة على شبكات "البوت" والتحكم بها. ويحتاج البرنامج الخبيث المُستخدَم للسيطرة على جهاز حاسوب يشكل جزءاً من شبكة البوت إلى استقبال التعليمات من المسيطر أو "راعي شبكات البوت" الذي يقوم بتجميعها. وللقيام بذلك يحتوي البرنامج الخبيث على قائمة طويلة من المواقع الإلكترونية التي لم يتم تسجيلها بعد باسم أحد، وفي وقت محدد مسبقاً تقوم كافة أجهزة الحاسوب التي تشكل جزءاً من شبكة البوت بمحاولة الاتصال بكل موقع إلكتروني، ويحاول راعي البوت نت مسبقاً تسجيل النطاقات من أعلى القائمة إلى أسفلها إلى أن يتمكن من شراء أحدها وإعداد الموقع لاستقبال الرسائل من شبكات البوت والرد عليها. ولكي يعطي راعي البوت نت هذا التكتيك فاعلية، عليه أن يستخدم حصراً نطاقات الدولة أو النطاقات الأخرى العالية المستوى التي لا تطلب إثبات الهوية لشراء موقع.

وبالإضافة إلى مشكلات الجرائم والتجسس والحرب الإلكترونية التي أصبحت ممكنة بسبب ضعف أمن نظام أسماء النطاقات، فإن النظام نفسه يحتوي ثغرات أمنية تجعله عرضة للهجوم. وفي عام 2008 أنشأ دان كامينسكي الخبير في أبحاث الأمن أداة برمجية بإمكانها تقديم معلومات مزيفة إلى نظام أسماء النطاقات والسيطرة على المواقع والبريد الإلكتروني وحركة شبكة الإنترنت. وكان بالإمكان توظيف هذا الهجوم لجني الأرباح أو تعطيل النظام بتقديم معلومات خاطئة على مستويات عالية.[14] وتمكّن الباحثون في

نظام أسماء النطاقات من التوصل إلى حل مؤقت، غير أن الثغرة الأساسية لاتزال موجودة ويمكن استغلالها من خلال هجمات أكثر تعقيداً.

كما يمكن تعطيل نظام أسماء النطاقات عن طريق شن هجوم شرس للحرمان من الخدمة كالذي استُخدِم في اختبار عام 2007 من قبل أفراد مجهولين. وفي تلك الحادثة تم إغراق ستة من أصل ثلاثة عشر نطاقاً عالية الأهمية بدفق من آلاف الطلبات في الثانية الواحدة. وتعطّل نطاقان لعدم قدرتهما على تحمل الزحام، ولكن المهاجمين أمروا جحافلهم الإلكترونية بالانسحاب بعد ثماني ساعات، ولو استمر هجومهم لكان أطاح ببقية الأنظمة.

ولمعالجة مشكلة أمن نظام أسماء النطاقات يجب العمل في مسارين منفصلين: مسار قانوني وتنظيمي من شأنه تصعيب مهمة المجرمين في تسجيل عناوين إلكترونية لأغراض غير مشروعة؛ ويوازيه مسار تقاني لتطبيق أمن نظام أسماء النطاقات (DNSSEC). ويتطلب المسار الأول تحرّك القائمين على تسجيل النطاقات الوطنية نحو تطبيق متطلبات تسجيل أشد صرامة للأفراد أو الشركات التي تريد شراء اسم نطاق. وحددت شركة "مكافي" McAfee المختصة بأمن الإنترنت نماذج مبادرات لتأمين تسجيل النطاقات الوطنية في أربعة بلدان هي: هونج كونج (.hk) وتشيلي (.cl) واليابان (.jp) وأيرلندا (.ie)،[15] حيث طبّق مسؤولو التسجيل في كل من هذه البلدان متطلبات أشد صرامة لتسجيل المواقع الإلكترونية، كما عملوا عن

كثب مع المراكز الوطنية للاستجابة لطوارئ الحاسب الآلي (CERTs) والشرطة والسلطات التنظيمية من أجل تحديد المواقع الخبيثة وإيقافها ومقاضاة القائمين على تشغيلها.

وطبقت تشيلي نظاماً يتطلب تأكيداً من بنك العميل للقيام بعملية شراء باستخدام بطاقة الائتمان، وباعتماد هذا الإجراء أصبح من الصعب استخدام أرقام بطاقات الائتمان المسروقة لشراء مواقع إلكترونية بأسماء وهمية، وتتحرك تشيلي بسرعة لإيقاف المواقع الخبيثة حال اكتشافها. كما أن أيرلندا ركزت جهودها على "إمكانية التتبع" حيث عملت على التحقق من هوية المسجلين والتأكد من أن لهم صلة شرعية في أيرلندا، وأن لهم حقوقاً شرعية في اسم النطاق الذي يسجلون فيه. ويجدر بدول الخليج النظر في تبني متطلبات مشابهة.

إن الانتقال إلى فئة أقل المخاطر لن يكون مهمة صعبة. وقد حددت مكافي 43 نطاقاً خطراً فقط في المملكة العربية السعودية و34 في دولة الإمارات العربية المتحدة. ومن الممكن التخلص من هذه المواقع ووضع قواعد ومعايير تدقيق جديدة لضبط المواقع الخطرة التي لم يتم التعرف عليها، ومنع تأسيس أي مواقع جديدة من هذا النوع، وذلك قبل إصدار ترتيب السنة القادمة.[16]

من الناحية التقانية، على دول الخليج التحرك باتجاه تبني استخدام امتداد النطاقات الأمنية التي من شأنها أن تتحقق من كل جزئية في حركة

نظام أسماء النطاقات، بدءاً من المستخدمين الأفراد الذين يطلبون مواقع إلكترونية حتى "الجذر" (قائمة مجال المستوى الأعلى لمخدمات نظام أسماء النطاق DNS servers) والعودة مرة أخرى إلى الأسفل. ولكي يعمل هذا النظام بشكل فعال يجب تحميل برنامج DNSSEC على كافة أجهزة الحاسوب، سواء كانت مخدمات أو أجهزة حاسوب محمولة أو هواتف ذكية.

وقامت هيئة الإنترنت للأسماء والأرقام المخصصة "الآيكان" (ICANN) التي تتولى إدارة ملف منطقة الجذر "بإدراج" الجذر في 15 تموز/ يوليو 2010 (أي أنها أنشأت توقيعاً رقمياً للدلالة على المصداقية). وطبقت أربع دول على الأقل نظام DNSSEC بشكل كامل لنطاقاتها العليا، ومن بين هذه الدول البرازيل وبلغاريا وجمهورية التشيك وبورتوريكو والسويد. كما تم مؤخراً إدراج النطاق (us.) بالإضافة إلى النطاق (biz.) من قبل مسجلها الشركة الأمريكية "نيوستار" ونطاقات (org.) (تم إدراجها في تموز/ يوليو 2008). وعلى دول مجلس التعاون لدول الخليج العربية التحرك بسرعة لوضع أسس اختبار لتطبيق نظام DNSSEC، وإعداد برامج لمساعدة الهيئات الحكومية وشركات القطاع الخاص في تطبيق هذا النظام.

التركيز على سلامة الشبكة

يستغل مجرمو الإنترنت والعابثون الآخرون ذوو النيات الخبيثة ضعف أنظمة الوقاية وتلوث بيئة الشبكة لشن هجماتهم. ونظراً للطبيعة العالمية للإنترنت فغالباً ما يكون مصدر أنظمة الهجوم مختلفاً عن مكان وجود الفرد

أو الأفراد الذين يتحكمون في الهجوم. إن أمن الشبكة الوطنية لا يرتبط بالضرورة بوجود مشكلات جريمة إلكترونية، إلا أن قياس مستوى الجريمة الإلكترونية يبين درجة تمتُّع الشبكة الوطنية ببيئة نظيفة تحول دون وقوع أنظمة الاستضافة ضحية للجرائم الإلكترونية أو التواطؤ من دون قصد مع منفذي هذه الجرائم.

ويمكن الرجوع إلى بعض التقارير الصادرة عن أهم الشركات لنسلِّط الضوء على أمن شبكة الإنترنت في دول الخليج. أشارت شركة "سيمانتك" Symantec في آخر تقرير لها حول تهديدات أمن الإنترنت في أوربا والشرق الأوسط وشمال إفريقيا *Internet Security Threat Report for Europe, the Middle East and Africa* إلى أن المملكة العربية السعودية تحتل المرتبة الأولى من حيث عدد الديدان الخبيثة على شبكتها، وقد تلتها في ذلك دولة الإمارات العربية المتحدة.[17] كما أن تصنيف مكافي السنوي للنطاقات العالمية من حيث المخاطر قد وضع نطاق المملكة العربية السعودية (sa.) في المرتبة 42، وجاء نطاق دولة الإمارات العربية المتحدة (ae.) في المرتبة 65 من بين 104 دول.[18]

وفي تقرير "مايكروسوفت لأمن المعلومات" *Microsoft Security Intelligence Report* في النصف الثاني من عام 2009 جاءت المملكة العربية السعودية في المرتبة السابعة ودولة الكويت في المرتبة 13 على قائمة الدول الأكثر إصابة بالبرمجيات الخبيثة. كما جاءت مملكة البحرين في المرتبة

15 والكويت في المرتبة 21 على قائمة الدول من حيث عدد الرسائل التطفلية (spam) التي يستقبلها مستخدم الإنترنت.

وتتمتع كافة دول مجلس التعاون بنسب أعلى مقارنة مع بقية العالم من حيث عدد المواقع الإلكترونية التي وقعت ضحية لهجمات حَقن لغة الاستعلامات البنيوية (SQL injection attacks). فخلال عام 2009 أصابت هجمات حقن لغة الاستعلامات البنيوية ما نسبته 0.011٪ من إجمالي المواقع الإلكترونية في العالم. بينما تعرضت المواقع الإلكترونية في دول الخليج بنسبة 0.81٪ لهجمات حقن لغة الاستعلامات البنيوية. ومقارنة ببقية دول العالم جاءت معدلات دول الخليج عالية جداً من حيث استقبالها لصفحات التحميل الخفي (drive-by download) والتي تقوم من دون لفت انتباه الضحية بتحميل برامج ضارة على حواسيب المستخدمين الذين يزورون هذه المواقع. وبلغت نسبة المواقع التي استقبلت صفحات التحميل الخفي في دول الخليج 0.672٪، بينما لم تتجاوز هذه النسبة 0.24٪ من المواقع حول العالم. إلا أن النطاق العُماني (om.) فاق كافة المنافسين في هذه الإحصائية حيث استقبل ما نسبته 1.58٪ من مواقعه الإلكترونية صفحات تحميل خفي، وجاءت دولة الكويت في المرتبة الثانية بمعدل أقل من النصف مقارنة بسلطنة عُمان. وفي دولة قطر تعد هجمات التصيُّد الإلكتروني (Phishing) خارجة عن نطاق السيطرة حيث يبلغ عدد مواقع التصيد 65 موقعاً في كل 1000 عملية استضافة على الإنترنت، بينما تبلغ هذه النسبة عالمياً 0.54٪. وتأتي معدلات المملكة العربية السعودية بنسبة 0.48٪ وهي أقل من المعدلات الدولية، كما أن

معدلات كل من مملكة البحرين ودولة الإمارات العربية المتحدة جاءت أقل من المعدلات الدولية بواقع 0.17٪ و0.05٪ على التوالي. وتعد دولة الكويت بنسبة 6.51٪ ودولة قطر بنسبة 2.77٪ الدولتين الوحيدتين اللتين جاء معدلاهما أعلى من المعدلات الدولية من حيث عدد مواقع توزيع البرامج الخبيثة لكل 1000 عملية استضافة على الإنترنت وبنسبة 1.3٪.

هذه الأرقام لا تنذر بالخطر، ففي الأنماط الأخرى من الهجمات كالأبواب الخلفية (backdoors) التي تسمح بالتسلل إلى الأنظمة بطرائق غير قانونية، جاءت المملكة المتحدة في المرتبة الأولى تلتها إسبانيا في المرتبة الثانية ثم ألمانيا في المرتبة الثالثة. وصنفت مكافي كلاً من المملكة العربية السعودية ودولة الإمارات العربية المتحدة ضمن فئة "المخاطر المنخفضة". وعلى رغم أن بيئة الشبكة في منطقة الخليج ليست الأسوأ، فإن هناك مجالاً للتحسين، وبخاصة في ضوء التوجهات التي ترجح نمو عدد مستخدمي الإنترنت في المنطقة.

إن مستويات استخدام الإنترنت في الشرق الأوسط أعلى بشكل طفيف من مثيلاتها في بقية العالم بنسبة 28.3٪ مقابل 25.5٪، إلا أن مستويات استخدام الحزمة العريضة (broadband) أقل من 10٪ في الشرق الأوسط بعامة، وبنسبة 7٪ في دول مجلس التعاون لدول الخليج العربية. وتتوقع مؤسسة تيليجيوغرافي، وهي مؤسسة رائدة في أبحاث الاتصالات، أن يتضاعف معدل استخدام الحزمة العريضة في الشرق الأوسط خلال

السنوات الأربع القادمة. ومما لا شك فيه أن هذا التوسع سيرافقه منافع اقتصادية، إلا أنه سيؤدي أيضاً إلى ارتفاع مستويات الإصابة بالفيروسات وزيادة عدد الأنظمة الموبوءة.

وربما يكون عدد مستخدمي الهواتف الجوالة الكبير سبباً لهذا القلق. وتتمتع دول مجلس التعاون لدول الخليج العربية بأعلى مستويات استخدام للهواتف الجوالة في العالم، بالإضافة إلى أن عديداً من المستخدمين ينتقلون إلى استخدام الهواتف الذكية التي تتيح الاتصال بالإنترنت. ويتوقع الباحثون في مجال الأمن أن تشكل الهواتف الجوالة الهدف الرئيسي للمتربصين الإلكترونيين في ظل تسارع وتيرة ارتفاع معدلات مستخدمي الهواتف الذكية.

أما فيما يتعلق بالسلامة العامة، فإن تحسين أمن الشبكة يتطلب أولاً جمع البيانات. لذا على مزودي خدمة الإنترنت في دول مجلس التعاون العمل عن كثب مع مراكز الاستجابة لطوارئ الحاسب الآلي (CERTs) والشركات الخاصة لمراقبة أمن الفضاء الإلكتروني للتمكن من القيام برصد فوري لأمن الشبكة، وإعداد تقارير فصلية وسنوية بناءً على هذه البيانات. ويمكن استخدام هذه التقارير لرسم الخط الأساسي للسنة الجارية، ووضع أهداف لتخفيف المشكلات في كل بلد عن كل فئة، إلا أن عملية الضبط هذه لا تقتصر على إعداد تقارير منمقة. وقد يتيح الوعي الظرفي على الشبكات

إمكانية تحديد حلول مباشرة لأي برمجيات ضارة أو شبكات "البوت" أو رسائل تطفلية أو أي أنشطة خبيثة أخرى.

بإمكان التقانة المتوافرة اليوم تحديد المشكلات على الشبكات الوطنية لحلها على الفور. وتقوم حالياً شركة "كومكاست" Comcast، وهي شركة لتزويد خدمة الإنترنت في الولايات المتحدة، بإعداد مشروع تجريبي ينبِّه المشتركين في حال تبيّن أن الحركة من أجهزتهم تبدو كجزء من شبكة "بوت" أو أن هناك أي مؤشر ينذر بأنه قد تم تحميل برنامج خبيث على أجهزتهم. كما تقدم كومكاست نصائح مجانية وأدوات لإزالة البرمجيات الخبيثة مع إرسال الإشعار، وفي نهاية المطاف قد تبدأ بحظر الأنظمة من الدخول على الشبكة. ويجب إلزام مزودي خدمة الإنترنت في دول مجلس التعاون لدول الخليج العربية بإعداد برامج مشابهة. وقد يكون من الحكمة التحقق من أن الأجهزة تقوم بتشغيل برامج مشروعة، وأنه يتم تحديث هذه البرامج، وأن الأنظمة تتمتع بتقنية فعّالة لمضادات الفيروسات ومضادات البرامج الخبيثة.

بالإمكان أيضاً إيقاف الأنشطة الخبيثة على الشبكة قبل وصولها إلى أجهزة تستضيفها بما يضاعف المشكلة. وباستطاعة تقنيات الفحص الدقيق للحزَم رصد الحركة على الشبكة لاستبعاد البرامج الخبيثة، وتستطيع التقانات الآن العمل بانتظام ومن دون تأخير، أي أن باستطاعتها العمل بنفس سرعة الإشارات التي تحمل حركة الإنترنت ولا تُسبب أي تأخير في حركة المعلومات على الشبكة. وبالإضافة إلى رصد البرمجيات الخبيثة المعروفة

وإيقافها، يمكن استخدام عملية التفتيش الدقيق للحزم لرصد أي حركة غريبة تشير إلى أي هجوم جديد من نوعه لم يتم رصده سابقاً.

إن الأخذ بهذه الخطوات مجتمعة من شأنه أن يحسّن بشكل كبير أمن الشبكة بين دول مجلس التعاون لدول الخليج العربية وسيجعل من مجلس التعاون منظمة تعاونية نموذجية في مجال الفضاء الإلكتروني. وعلى رغم أن هذه الإجراءات لن تكون عصيّة على الاختراق، فإنها ستتمكن مجتمعة من إيقاف 99٪ من الهجمات التي تعتمد على جوانب الضعف المعروفة.

التعاون لمكافحة الجرائم الإلكترونية

ليس بإمكان الحلول التقانية وحدها أن تعالج بشكل كاف جميع مشكلات الجريمة الإلكترونية والتهديدات الأخرى التي تحيق بالفضاء الإلكتروني، فالأنظمة والتحقيقات والإجراءات القانونية ضرورية أيضاً. ونظراً إلى قدرة المهاجمين في بلد ما على استهداف الأنظمة في بلد آخر، فلا بد من وضع آليات تتيح إمكانية التحقيق والمقاضاة دولياً. كما يجب على البلدان وضع آليات للتعامل مع طلبات إغلاق الشبكات في وجه الأنظمة التي يتم رصدها، من حيث هي أطراف مشاركة في هجمات الحرمان من الخدمة أو أي نمط آخر من الهجمات. وعلى دول مجلس التعاون لدول الخليج العربية أن تدرس توقيع معاهدة المجلس الأوربي حول جرائم الشبكات الإلكترونية والمصادقة عليها، أو القيام في خيار بديل لها بالدخول في معاهدة شبيهة تضم

دول مجلس التعاون أو دول الشرق الأوسط بصورة أوسع، ثم التفاوض حول اتفاقية تبادلية مع المجلس الأوربي.

الاستثمار في تخفيف آثار هجمات الحرمان من الخدمة

ليس من حل قاطع وحيد لمنع هجمات الحرمان من الخدمة، إلا أنه من الضروري اتباع استراتيجية متعددة المحاور يكون أساسها التركيز على إيقاف الهجمات على الشبكة قبل وصولها إلى الأنظمة المستهدفة. إن الميزة المؤذية التي تتمتع بها هجمات الحرمان من الخدمة تستمد قوتها من إمكانية استخدام عدة أنظمة لاستهداف نظام واحد. ويمكن انتهاج تكتيك على شبكة الإنترنت من أجل إيقاف هذه الهجمات للقضاء على هذه الميزة، وذلك بتبديدها عند عدة نقاط. فمع أن أكبر شبكة "بوت" تستطيع إغراق الأنظمة بتسونامي من البيانات يقارب 120 جيجابايت في الثانية، وهو يفوق إلى حد كبير قدرة استيعاب أي شبكة خاصة، إلا أن هذا الكم من البيانات لا يشكل قطرة في محيطات الشبكة الوطنية المترامية الأطراف. لذا تجب إزاحة مسؤولية إيقاف هجمات الحرمان من الخدمة عن كاهل المستهدفين لتصبح من اختصاص مشغلي شبكة الإنترنت.

وفي الولايات المتحدة الأمريكية يقوم عديد من مزودي خدمة الإنترنت بتقديم إجراء تخفيف لهجمات الحرمان من الخدمة في جزء من "خدمات الأمن التي تديرها"، وهي خدمة استثنائية تُقدَّم للمشتركين لقاء

رسم إضافي. ولتخفيف هجمات الحرمان من الخدمة، تقوم هذه الخدمات بمراقبة الحركة ورصد التهديدات وتصفية الحزم التي يتضح أنها جزء من هجوم والسماح بمرور الحركة التي لا تشكل تهديداً، وإخضاع الحزم التي لا يمكن تصنيفها ضمن أي من الفئتين لمستويات تحليل أشد صرامة قبل تمرير البيانات النظيفة إلى وجهتها. وعلى دول مجلس التعاون لدول الخليج العربية تشجيع مزودي خدمة الإنترنت فيها على تقديم خدمات مشابهة لكافة مشتركيها شركاتٍ أو أفراداً.

وتنبع الصعوبة الحقيقية في مواجهة تنفيذ هذه الاستراتيجية من التنسيق المطلوب بين مزودي خدمة الإنترنت من جهة، ومالكي الأنظمة المستهدفة من جهة أخرى. ويجب أن يتم التنسيق بشكل فوري تقريباً، ويتطلب قيام مزودي خدمة الإنترنت بالتعامل جدياً مع التهديد، وهو أمر لم يقتنع مزودو خدمة الإنترنت في الولايات المتحدة بالقيام به حتى الآن. وفي خطوة أولى، على مزودي الخدمة والمستخدمين التعاون فيما بينهم لترسيخ إدراك الموقف situational awareness. وعادة ما تقوم هجمات الحرمان من الخدمة بإغراق الشبكات المستهدفة بنوع واحد من الزحام، كطلب صفحة إنترنت بشكل متكرر على سبيل المثال. لذا فإن الخطوة الأولى لرصد هجوم حرمان من الخدمة يجب أن تبدأ بالتعرف على الموجات الغريبة لنوع مرور معين. وحال رصد الحزم الغريبة يجب أن تعمل الأنظمة المستهدَفة بشكل فوري وبالتنسيق مع مزودي خدمة الإنترنت على محاصرة الهجمات واستبعادها والسماح للحزم السليمة بالعبور.

ويمكن إعداد وضبط مكونات الشبكة لتطلب إقراراً بخصوص الحزم المرسَلة حال حدوث هجوم حرمان من الخدمة، وبالتالي لا تستطيع الأنظمة التي تشن الهجوم بدء الإرسال من دون إتمام عملية إنشاء ارتباط متبادل. كما أنه باستطاعة مزودي خدمة الإنترنت اتخاذ خطوات لكبح الحزم التي تحمل عناوين بروتوكول إنترنت زائفة، كالعناوين الخاصة أو عناوين بروتوكول الإنترنت التي لم يتم تخصيصها بعد.

تعزيز البنى التحتية الحساسة ضد الهجمات الإلكترونية

في دول مجلس التعاون لدول الخليج العربية ثلاثة أنواع من البنى التحتية التي تجب حمايتها مهما كلف الأمر، وهي: مرافق استخراج النفط والغاز، ومولدات الكهرباء، ومحطات تحلية المياه. ولحماية البنية التحتية الحساسة من الهجمات الإلكترونية، على دول مجلس التعاون أن تركز جهودها حول ثلاثة محاور، وهي: 1) الحد من إمكانية الاتصال؛ 2) وجوب تشفير وترميز كافة أنظمة التحكم؛ 3) استبقاء وصيانة أجهزة التحكم اليدوية. ويجب اختبار وتدقيق مستوى الأمن في هذه النواحي بشكل دائم للتأكد من الالتزام بكافة التعليمات.

ويتضمن الحد من إمكانية الاتصال؛ فصل مكونات هذه الأنظمة عن شبكة الإنترنت العامة، إذ يمكن استخدام الاتصال بالشبكة للولوج إلى أنظمة حساسة، وبالتالي التحكم والتلاعب بهذه الأنظمة. وقد يدّعي معظم مرافق الخدمات عدم اتصال أنظمتها بشبكة الإنترنت العامة، ومع ذلك

تحدث حالات تطفل باستخدام الإنترنت. وقد أظهرت مجلة وول ستريت جورنال الأمريكية في تقرير صدر عنها عام 2009 أن وكالات استخبارات أجنبية تمكنت من الدخول إلى شبكة الكهرباء الأمريكية وزرعت فيها "قنابل منطقية" (logic bombs) يمكن ضبطها على توقيت محدد لتدمير النظام. وفي عام 2009 أشار برنامج التقارير الإخبارية **60 دقيقة** "*60 Minutes*" إلى قيام بعض المخرّبين بتعطيل شبكة الكهرباء في أحد بلدان أمريكا الجنوبية.

وفي أغلب الحالات يقوم مصنعو المعدات بالاتصال بشبكة الإنترنت للقيام بفحوصات عن بعد. وتستخدم بعض المرافق في الولايات المتحدة وأوربا الإنترنت للتحكم بأنظمتها في نوع من تخفيض التكاليف. وفي حالات أخرى تم الدخول عبر هواتف الصوت عبر الإنترنت (VoIP) التي تم تحميلها في غرف التحكم. وللتحقق من حالات الاتصال بالإنترنت يجب إجراء تدقيق دوري للأنظمة وتأسيس "الفِرق الحمراء" لإجراء اختبارات بمحاولة اختراق الأنظمة.

ولا تعد الأنظمة غير المتصلة بالإنترنت منيعة ضد الهجمات الإلكترونية، فعلى رغم أن قطْع الاتصال بالإنترنت سيمنع المهاجمين من شن هجماتهم عن بعد، فإن ذلك لن يمنعهم من شن الهجمات باستخدام وسائل أخرى. فبالإمكان دسّ البرمجيات الخبيثة في الوسائط المحمولة، مثل سواقات الناقل التسلسلي العام (USB) والأقراص المدمجة التي يتم استخدامها لتحديث الأنظمة. ويمكن اختراق الشبكة والتحكم فيها عبر

الارتباط بالشبكات، والاستيلاء أو إعادة البث على الموجات الصغرى وموجات البث الأخرى، أو إنشاء نقاط ربط خفية مع الشبكة العامة. وهذا لا يعني أن إزالة الارتباط بالإنترنت أمر غير مجدٍ، فإذا تعذّر على المهاجمين دخول الأنظمة عبر الإنترنت سيضطرون إلى الاقتراب فعلياً من الأنظمة، ما سيزيد من احتمالات ضبطهم وتعريض أنفسهم للخطر. إلا أن الحد من الاتصال بالإنترنت لا يغطي سوى جانب واحد من جوانب الأمن، لذا يجب تشفير كافة الحزم على الشبكة، وعدم السماح بالدخول إلى الشبكة إلا بموجب مصادقة متعددة العوامل.

وأخيراً، وتحسباً لفشل هذه الإجراءات الأمنية يجب أن يتمتع القائمون على تشغيل هذه البنى التحتية الحساسة بالقدرة على العودة إلى استخدام أجهزة التحكم اليدوية التي لا تتطلب الاعتماد على التقانات والنظُم الرقمية والبرامج المؤتمتة، ولاتزال إمكانية التغيير إلى الدعم اليدوي متاحة في معظم الصناعات، إلا أن الأنظمة الحديثة لا يمكن تشغيلها في حال تعطلت أجهزة التحكم الإلكترونية الخاصة بها أو تم استغلالها من قبل العابثين الذين يضمرون السوء.

تحصين الأنظمة الحكومية والعسكرية

كما هي الحال بالنسبة للبنى التحتية الحساسة، على الأنظمة الحكومية والعسكرية الحد من الاتصال بالإنترنت وفصل الأنظمة الحساسة بشكل تام

عن الأنظمة المتصلة بالإنترنت. ويجب عند بوابات الإنترنت معاينة كل حركة بحثاً عن أنماط الهجوم المعروفة، كما يجب استخدام برامج رصد الحزم الغريبة لضبط أي أنماط مشبوهة. ويجب رصد كافة المعلومات التي تخرج من الشبكات الحكومية وتحليلها بغرض ضبط تسريب المعلومات غير المصرح بها. كما يجب استخدام الأنظمة داخل محيط الشبكات لمراقبة وضبط وتحليل تدفق المعلومات بحثاً عن أنماط مشبوهة في سلوكيات الشبكة. وتنبغي حماية كافة أجهزة الحاسوب التي تعمل على هذه الشبكات باعتبارها أصولاً خاصة، وذلك باستخدام برامج منع الاختراق ومكافحة الفيروسات والبرمجيات الخبيثة. وعلى كافة مستخدمي هذه الأنظمة تطبيق المصادقة بعاملين على الأقل. كما يجب تقسيم شبكات الإنترنت إلى شبكات فرعية بحيث يُمنَح إذن الدخول حسب الحاجة فقط.

الخاتمة

لتخفيف التهديدات وسدّ مواضع الضعف وإدارة النتائج في الفضاء الإلكتروني، على دول مجلس التعاون لدول الخليج العربية التحرك باتجاه اعتماد أجندة موحدة للأمن الإلكتروني. وللمباشرة بهذه الأجندة على دول مجلس التعاون أن تؤسس لجنة توجيهية رفيعة المستوى تضم ممثلين من هيئات تنظيم الاتصالات، ومراكز الاستجابة لطوارئ الحاسب الآلي، والشرطة الوطنية والجيش، والقائمين على تسجيل النطاقات، ومزودي خدمة

الإنترنت، ومشغلي البنى التحتية الحساسة من كل دولة من الدول الأعضاء. وعلى هذه اللجنة بدورها أن تشكل سلسلة من المجموعات الفرعية لمعالجة كل موضوع على الأجندة، بدءاً بتحسين أمن نظام أسماء النطاقات وانتهاءً بتأمين الأنظمة الحكومية والعسكرية. وعندما يتعلق الأمر بجوانب مثل البنية التحتية الحساسة والأنظمة الحكومية والعسكرية، على اللجنة أن تركز فقط على تبادل أفضل الممارسات المتبعة لمعالجة الهموم الأمنية لكل بلد.

أما فيما يتعلق بالجوانب الأخرى كأمن نظام أسماء النطاقات وتحسين وضع الشبكة ومكافحة الجرائم الإلكترونية وتخفيف هجمات الحرمان من الخدمة فيجب تكليف اللجان الفرعية بإعداد خطة استراتيجية مدتها خمس سنوات لتحسين الأمن بشكل ملموس بأسلوب تعاوني. إن الاستثمار البشري والمادي المناسب في هذا الاتجاه من شأنه أن يبدأ بتحسين أمن الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية، مما سيجعل المنطقة مثالاً تحتذي به بقية دول العالم.

الهوامش

1. انظر:

Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," *PBS Frontline*, February 26, 2010 (http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-thc-net-irans-cyber-army.html).

2. انظر:

Camille Tuutti, "Iranian Cyber Army Second Largest in the World, Claims Iranian Commander," thenewnewinternet. com, Friday, May 21, 2010 (http://www.thenewnewinternet.com/2010/05/21/iranian-cyber-army-second-largcst-in-the-world-claims-iranian-commander).

3. انظر:

"Iranian Cyber Warfare Threat Assessment," *Defense Tech*, September 23, 2008 (http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment).

4. .Rezvaniyeh, op. cit.,

5. .Ibid

6. انظر:

Emma Woollacott, "Baidu: Hacking war Breaks out Between Iran and China," *TG Daily*, January 12, 2010 (http://www. tgdaily.com/security-features/45454-hacking-war-breaks-out-between-iran-and-china).

7. انظر:

Kevin Coleman, "Wikileaks Fiasco Exposes Gaping Holes in Cyber Domain," *Defense Tech*, August 9, 2010 (http://defensetech.org/category/cyber-warfare/#ixzz0rIe51Zv0).

8. انظر:

Simon McGregor-Wood, "Is Isracl Already at War With Iran? Experts Bclieve Israeli Security Forces are Hacking into Iranian Networks," *ABC News International*, July 8, 2009 (http://abcnews.go.com/International/story?id=8030578&page=1).

9. Ibid.

10. Ibid.

11. انظر:

Mustapha Ajbaili, "Saudi and UAE at High Risk to Cyber-Crime: Report," *Al Arabiya News Channel*, November 15, 2009 (http://www. alarabiya.net/articles/2009/11/15/91411. html).

12. انظر:

Vineetha Menon, "UAE Cybercrime Squad Gunning Forward," *Arabian Business*, April 23, 2009 (http://www.arabianbusiness.com/553470-uae-cybercrime-squad-gunning-forward).

13. انظر:

Andy Sambridge, "Abu Dhabi Police Warns of Online Fraud," *ITP.net*, March 22, 2010 (http://www.itp.net/579 675-abu-dhabi-police-warns-of-online-fraud).

14. انظر:

Center for Strategic and International Studies (CSIS), "Cyber Security for the 44th Presidency: Telecommunications Task Group Final Report," October 28, 2008.

15. انظر:

McAfee, "Mapping the Mal Web: The World's Riskiest Domains," December 2009 (us.mcafee.com/en-us/local/docs/Mapping_Mal_Web. pdf), 23.

16. Ibid., 12–13.

17. انظر:

Symantec Enterprise Security, "Symantec Internet Security Threat Report: Regional Data Sheet – Europe, Middle East, and Africa," April, 2010 (http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_emea_internet_security_threat_report_xv_04-2010.en-us.pdf).

18. McAfee, op. cit.

المراجع

Ajbaili, Mustapha. "Saudi and UAE at High Risk to Cyber-Crime: Report." Al Arabiya News Channel, November 15, 2009 (http://www.alarabiya.net/articles/2009/11/15/91411.html).

Center for Strategic and International Studies (CSIS). "Cyber Security for the 44th Presidency: Telecommunications Task Group Final Report." October 28, 2008.

Coleman, Kevin. "Wikileaks Fiasco Exposes Gaping Holes in Cyber Domain." Defense Tech, August 9, 2010 (http://defensetech.org/category/cyber-warfare/#ixzz0rIe51Zv0)

"Iranian Cyber Warfare Threat Assessment." Defense Tech, September 23, 2008 (http://defensetech.org/2008/09/23/ iranian-cyber-warfare-threat-assessment).

McAfee. "Mapping the Mal Web: The World's Riskiest Domains." December 2009 (us.mcafee.com/en-us/local/docs/ Mapping_Mal_Web.pdf).

McGregor-Wood, Simon. "Is Israel Already at War With Iran? Experts Believe Israeli Security Forces Are Hacking Into Iranian Networks." ABC News International, July 8, 2009 (http://abcnews.go.com/International/story?id=8030578& page=1).

Menon, Vineetha. "UAE Cybercrime Squad Gunning Forward." Arabian Business, April 23, 2009 (http://www.arabianbusiness.com/553470-uae-cybercrime-squad-gunning-forward).

Rezvaniyeh, Farvartish. "Pulling the Strings of the Net: Iran's Cyber Army." PBS Frontline, February 26, 2010 (http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html).

Sambridge, Andy. "Abu Dhabi Police Warns of Online Fraud." ITP.net, March 22, 2010 (http://www.itp.net/579675-abu-dhabi-police-warns-of-online-fraud).

Symantec Enterprise Security. "Symantec Internet Security Threat Report: Regional Data Sheet – Europe, Middle East, and Africa." April 2010

(http://eval.symantec.com/mktginfo/enterprise/white_papers/b-white paper_emea_internet_security _threat_report_xv_04-2010.en-us.pdf).

Tuutti, Camille. "Iranian Cyber Army Second Largest in the World, Claims Iranian Commander." Thenewnewinternet. com, May 21, 2010 (http:// www.Thenewnewinternet.com/2010/05/21/iranian-cyber-army-second-largest-in-the-world-claims-iranian-commander).

Woollacott, Emma. "Baidu: Hacking war Breaks out Between Iran and China." TG Daily, January 12, 2010 (http://www.tgdaily.com/ security-features/45454-hacking-war-breaks-out-between-iran-and-china).

نبذة عن المحاضرين

ريتشارد كلارك خبير معروف دولياً في مجال الأمن، بما فيه الأمن الداخلي والأمن القومي وأمن الفضاء الإلكتروني (الإنترنت) ومكافحة الإرهاب. وهو حالياً استشاري على الهواء لقناة إيه بي سي نيوز، ويقوم بالتدريس في معهد كنيدي لشؤون الحكم التابع لجامعة هارفارد.

شغل السيد كلارك منصب مستشار أول للبيت الأبيض في عهود آخر ثلاثة رؤساء للولايات المتحدة الأمريكية، وخلال أحد عشر عاماً من الخدمة المتواصلة غير المسبوقة في البيت الأبيض تولّى منصب المساعد الخاص للرئيس في الشؤون العالمية ومنصب المنسق القومي للأمن ومكافحة الإرهاب، بالإضافة إلى منصب المستشار الخاص للرئيس لأمن الفضاء الإلكتروني.

وقبل خدمته في البيت الأبيض، خدم لمدة 19 عاماً في وزارة الدفاع (البنتاجون) ووكالة الاستخبارات ووزارة الخارجية. وفي عهد إدارة ريجان شغل منصب نائب مساعد وزير الخارجية لشؤون الاستخبارات. أما في عهد إدارة جورج بوش الأب فقد شغل منصب مساعد وزير الخارجية للشؤون السياسية-العسكرية، وقام بتنسيق الجهود الدبلوماسية لدعم حرب الخليج عام 1990-1991 والترتيبات الأمنية التي أعقبتها.

يقوم السيد كلارك، بصفته شريكاً في مؤسسة غود هاربر، بتقديم الاستشارات للعملاء حول عدد من القضايا التي تشمل: إدارة المخاطر الأمنية للشركات وتقانة أمن المعلومات ومكافحة الإرهاب وتقديم المشورة إلى الحكومة الفيدرالية بشأن قضايا الأمن وتقنية المعلومات.

روبرت نيك زميل العلاقات الدولية المقيم في مجلس العلاقات الدولية ويقوم بدراسة حرب الفضاء الإلكتروني، ويعمل حالياً على تقرير خاص من المجلس يُعنى بحوكمة وأمن الإنترنت. وقبل زمالته، شغل منصب المدير في غود هاربر، وهي مؤسسة للاستشارات الأمنية-الاستراتيجية ولها مكاتب في العاصمة واشنطن وفي بوسطن بماساشوستس وفي أبوظبي بدولة الإمارات العربية المتحدة، حيث يقدِّم خدماته للعملاء المحليين والخارجيين حول مشروعات أمن الفضاء الإلكتروني والأمن الوطني.

وكان خلال الحملة الانتخابية للرئاسة الأمريكية عام 2008 قد قام بتنسيق فرقة مكافحة الإرهاب لحملة أوباما كما عمل في فرقة الأمن الوطني. وبعد انتخاب أوباما عمل في الفريق الرئاسي الانتقالي في وزارة الأمن الوطني الأمريكي وأصدر التقرير الختامي لفريق مراجعة الوكالة.

انضم روبرت نيك إلى مؤسسة غود هاربر بعد حصوله على ماجستير من معهد كنيدي لشؤون الحكم التابع لجامعة هارفارد. وكتب كثيراً عن قضايا أمن الفضاء الإلكتروني ومكافحة الإرهاب والأمن الوطني. وفي عام 2006 أخرج مع ستيفن سيمون تقرير القوة الضاربة لمؤسسة القرن بعنوان "الوطن المنسي". كما ألّف (بالاشتراك مع ريتشارد كلارك) كتاب **حرب الفضاء الإلكتروني: التهديد المقبل للأمن القومي وكيفية التصرف حياله** (2010).

صــدر من سلسلــة
محاضرات الإمارات

1. بريطانيا والشرق الأوسط: نحو القرن الحادي والعشرين

مالكولم ريفكند

2. حركات الإسلام السياسي والمستقبل

د. رضوان السيد

3. اتفاقية الجات وآثارها على دول الخليج العربية

محمد سليم

4. إدارة الأزمـات

د. محمد رشاد الحملاوي

5. السياسة الأمريكية في منطقة الخليج العربي

لينكولن بلومفيلد

6. المشكلة السكانية والسلم الدولي

د. عدنان السيد حسين

7. مسيرة السلام وطموحـات إسرائيل في الخليج

د. محمد مصلح

8. التصور السياسي لدولة الحركات الإسلامية

خليل علي حيدر

9. الإعلام وحرب الخليج: رواية شاهد عيان

بيتر آرنيت

10. الشورى بين النص والتجربة التاريخية

د. رضوان السيد

11. مشكلات الأمن في الخليج العربي
منذ الانسحاب البريطاني إلى حرب الخليج الثانية

د. جمال زكريا قاسم

12. التجربة الديمقراطية في الأردن: واقعها ومستقبلها

هاني الحوراني

13. التعليم في القرن الحادي والعشرين

د. جيرزي فياتر

14. تأثير تكنولوجيا الفضاء والكومبيوتر على أجهزة الإعلام العربية

محمد عارف

15. التعليم ومشاركة الآباء بين علم النفس والسياسة

دانييل سافران

16. أمن الخليج وانعكاساته على دول مجلس التعاون لدول الخليج العربية

العقيد الركن/ محمد أحمد آل حامد

17. الإمارات العربية المتحدة «آفاق وتحديات»

نخبة من الباحثين

18. أمن منطقة الخليج العربي من منظور وطني

صاحب السمو الملكي الفريق أول ركن

خالد بن سلطان بن عبدالعزيز آل سعود

19. السياسة الأمريكية في الشرق الأوسط والصراع العربي ـ الإسرائيلي

د. شبلي تلحمي

20. العلاقات الفلسطينية ـ العربية من المنفى إلى الحكم الذاتي

د. خليل شقاقي

21. أساسيات الأمن القومي: تطبيقات على دولة الإمارات العربية المتحدة

د. ديفيد جارنم

22. سياسات أسواق العمالة في دول مجلس التعاون لدول الخليج العربية

د. سليمان القدسي

23. الحركات الإسلامية في الدول العربية

خليل علي حيدر

24. النظام العالمي الجديد

ميخائيل جورباتشوف

25. العولمة والأقلمة: اتجاهان جديدان في السياسات العالمية

د. ريتشارد هيجوت

26. أمن دولة الإمارات العربية المتحدة: مقترحات للعقد القادم

د. ديفيد جارنم

27. العالم العربي وبحوث الفضاء: أين نحن منها؟

د. فاروق الباز

28. الأوضاع الاقتصادية والسياسية والأمنية في روسيا الاتحادية

د. فكتور ليبيديف

29. مستقبل مجلس التعاون لدول الخليج العربية

د. ابتسام سهيل الكتبي
د. جمال سند السويدي
اللواء الركن حيي جمعة الهاملي
سعادة السفير خليفة شاهين المرر
د. سعيد حارب المهيري
سعادة سيف بن هاشل المسكري
د. عبدالخالق عبدالله
سعادة عبدالله بشارة
د. فاطمة سعيد الشامسي
د. محمد العسومي

30. الإسلام والديمقراطية الغربية والثورة الصناعية الثالثة: صراع أم التقاء؟

د. علي الأمين المزروعي

31. منظمة التجارة العالمية والاقتصاد الدولي

د. لورنس كلاين

32. التعليم ووسائل الإعلام الحديثة وتأثيرهما في المؤسسات السياسية والدينية

د. ديل إيكلمان

33. خمس حروب في يوغسلافيا السابقة

اللورد ديفيد أوين

34. الإعلام العربي في بريطانيا

د. سعد بن طفلة العجمي

35. الانتخابات الأمريكية لعام 1998

د. بيتر جوبسر

36. قراءة حديثة في تاريخ دولة الإمارات العربية المتحدة

د. محمد مرسي عبدالله

37. أزمة جنوب شرقي آسيا: الأسباب والنتائج

د. ريتشارد روبيسون

38. البيئة الأمنية في آسيا الوسطى

د. فريدريك ستار

39. التنمية الصحية في دولة الإمارات العربية المتحدة من منظور عالمي

د. هانس روسلينج

40. الانعكاسات الاستراتيجية للأسلحة البيولوجية والكيماوية على أمن الخليج العربي

د. كمال علي بيوغلو

41. توقعات أسعار النفط خلال عام 2000 وما بعده ودور منظمة الأوبك

د. إبراهيم عبدالحميد إسماعيل

42. التجربة الأردنية في بناء البنية التحتية المعلوماتية

د. يوسف عبدالله نصير

43. واقع التركيبة السكانية ومستقبلها في دولة الإمارات العربية المتحدة

د. مطر أحمد عبدالله

44. مفهوم الأمن في ظل النظام العالمي الجديد

عدنان أمين شعبان

45. دراسات في النزاعات الدولية وإدارة الأزمة

د. ديفيد جارنم

46. العولمة: مشاهد وتساؤلات

د. نايف علي عبيد

47. الأسرة ومشكلة العنف عند الشباب
(دراسة ميدانية لعينة من الشباب في جامعة الإمارات العربية المتحدة)

د. طلعت إبراهيم لطفي

48. النظام السياسي الإسرائيلي: الجذور والمؤسسات والتوجهات

د. بيتر جوبسر

49. التنشئة الاجتماعية في المجتمع العربي في ظروف اجتماعية متغيرة

د. سهير عبدالعزيز محمد

50. مصادر القانون الدولي: المنظور والتطبيق

د. كريستوف شرور

51. الثوابت والمتغيرات في الصراع العربي ـ الإسرائيلي وشكل الحرب المقبلة

اللواء طلعت أحمد مسلم

52. تطور نظم الاتصال في المجتمعات المعاصرة

د. راسم محمد الجمال

53. التغيرات الأسرية وانعكاساتها على الشباب الإماراتي: تحليل سوسيولوجي

د. سعد عبدالله الكبيسي

54. واقع القدس ومستقبلها في ظل التطورات الإقليمية والدولية

د. جواد أحمد العناني

55. مشكلات الشباب: الدوافع والمتغيرات

د. محمود صادق سليمان

56. محددات وفرص التكامل الاقتصادي بين دول مجلس التعاون لدول الخليج العربية

د. محمد عبدالرحمن العسومي

57. الرأي العام وأهميته في صنع القرار

د. بسيوني إبراهيم حمادة

58. جذور الانحياز:
دراسة في تأثير الأصولية المسيحية في السياسة الأمريكية تجاه القضية الفلسطينية

د. يوسف الحسن

59. ملامح الاستراتيجية القومية في النهج السياسي
لصاحب السمو الشيخ زايد بن سلطان آل نهيان
رئيس دولة الإمارات العربية المتحدة

د. أحمد جلال التدمري

60. غسل الأموال: قضية دولية

مايكل ماكدونالد

61. معضلة المياه في الشرق الأوسط

د. غازي إسماعيل ربابعة

62. دولة الإمارات العربية المتحدة: القوى الفاعلة في تكوين الدولة

د. جون ديوك أنتوني

63. السياسة الأمريكية تجاه العراق

د. جريجوري جوز الثالث

64. العلاقات العربية ـ الأمريكية من منظور عربي: الثوابت والمتغيرات

د. رغيد كاظم الصلح

65. الصهيونية العالمية وتأثيرها في علاقة الإسلام بالغرب

د. عبدالوهاب محمد المسيري

66. التوازن الاستراتيجي في الخليج العربي خلال عقد التسعينيات

د. فتحي محمد العفيفي

67. المكون اليهودي في الثقافة المعاصرة

د. سعد عبدالرحمن البازعي

68. مستقبل باكستان بعد أحداث 11 أيلول/ سبتمبر 2001
وحرب الولايات المتحدة الأمريكية في أفغانستان

د. مقصود الحسن نوري

69. الولايات المتحدة الأمريكية وإيران: تحليل العوائق البنيوية للتقارب بينهما

د. روبرت سنايدر

70. السياسة الفرنسية تجاه العالم العربي

شارل سان برو

71. مجتمع دولة الإمارات العربية المتحدة: نظرة مستقبلية

د. جمال سند السويدي

72. الاستخدامات السلمية للطاقة النووية: مساهمة الوكالة الدولية للطاقة الذرية

د. محمد البرادعي

73. ملامح الدبلوماسية والسياسة الدفاعية لدولة الإمارات العربية المتحدة

د. وليم رو

74. الإسلام والغرب عقب 11 أيلول/ سبتمبر: حوار أم صراع حضاري؟

د. جون إسبوزيتو

75. إيران والعراق وتركيا: الأثر الاستراتيجي في الخليج العربي

د. أحمد شكارة

76. الإبحار بدون مرساة المحددات الحالية للسياسة الأمريكية في الخليج العربي

د. كلايف جونز

77. التطور التدريجي لمفاوضات البيئة الدولية: من استوكهولم إلى ريو دي جانيرو

مارك جيدوبت

78. اقتصـادات الخليـج العـربي: التحديات والفرص

د. إبراهيم عويس

79. الإسلام السياسي والتعددية السياسية من منظور إسلامي

د. محمد عمارة

80. إحصاءات الطاقة: المنهجية والنماذج الخاصة بوكالة الطاقة الدولية

جون دينمان و ميكي ريسي و سوبيت كاربوز

81. عمليات قوات الأمم المتحدة لحفظ السلام: تجربة أردنية

السفير عيد كامل الروضان

82. أنماط النظام والتغيرات في العلاقات الدولية: الحروب الكبرى وعواقبها

د. كيتشي فوجيوارا

83. موقف الإسلاميين من المشكلة السكانية وتحديد النسل

خليل علي حيدر

84. الدين والإثنية والتوجهات الأيديولوجية في العراق: من الصراع إلى التكامل

د. فالح عبدالجبار

85. السياسة الأمريكية تجاه الإسلام السياسي

جراهام فولر

86. مكانة الدولة الضعيفة في منطقة غير مستقرة: حالة لبنان

د. وليد مبارك

87. العلاقات التجارية بين مجلس التعاون لدول الخليج العربية والاتحاد الأوربي: التحديات والفرص

د. رودني ويلسون

88. احتمالات النهضة في "الوطن العربي"
بين تقرير التنمية الإنسانية العربية ومشروع الشرق الأوسط الكبير

د. نادر فرجاني

89. تداعيات حربي أفغانستان والعراق على منطقة الخليج العربي

د. أحمد شكارة

90. تشكيل النظام السياسي العراقي: دور دول مجلس التعاون لدول الخليج العربية

جيمس راسل

91. الاستراتيجية اليابانية تجاه الشرق الأوسط
بعد أحداث الحادي عشر من سبتمبر

د. مسعود ضاهر

92. الاستخبارات الأمريكية بعد الحادي عشر من سبتمبر: سد الثغرات

إيلين ليبسون

93. الأمم المتحدة والولايات المتحدة والاتحاد الأوربي والعراق:
تحديات متعددة للقانون الدولي

ديفيد م. مالون

94. الحرب الأمريكية على الإرهاب وأثرها على العلاقات الأمريكية - العربية

جيمس نويز

95. القضية الفلسطينية وخطة الانفصال عن غزة:
آفاق التسوية.. انفراج حقيقي أم وهمي؟

د. أحمد الطيبي ومحمد بركة

96. حرب الولايات المتحدة الأمريكية على العراق
وانعكاساتها الاستراتيجية الإقليمية

د. أحمد شكارة

97. سيناريوهات المستقبل المحتملة في العراق

كينيث كاتزمان

98. الأسلحة النووية في جنوب آسيا

كريس سميث

99. العلاقات الروسية مع أوربا والولايات المتحدة الأمريكية
انعكاسات على الأمن العالمي

فيتالي نومكن

100. تقنيات التعليم وتأثيراتها في العملية التعليمية:
دراسة حالة كلية العلوم الإنسانية والاجتماعية بجامعة الإمارات العربية المتحدة

د. مي الخاجة

101. الخليج العربي واستراتيجية الأمن القومي الأمريكي

لورنس كورب

102. مواجهة التحدي النووي الإيراني

جاري سمور

114. الولايات المتحدة الأمريكية وأوربا في الشرق الأوسط وخارجه:
شركاء أم متنافسون؟

تشارلز كوبتشان

115. تعاظم دور حلف الناتو في الشرق الأوسط "الكبير"

فيليب جوردن

116. مكافحة الجرائم المعلوماتية وتطبيقاتها
في دول مجلس التعاون لدول الخليج العربية

د. ناصر بن محمد البقمي

117. ما مدى قدرة إيران على تطوير المواد الخاصة بالأسلحة النووية وتقنياتها؟

جـون لارج

118. السلام الهش في سريلانكا

كريس سميث

119. البرنامج النووي الإيراني:
الانعكاسات الأمنية على دولة الإمارات العربية المتحدة ومنطقة الخليج العربي

ريتشارد رسل

120. أمن الخليج وإدارة الممرات المائية الإقليمية:
الانعكاسات على دولة الإمارات العربية المتحدة

برتراند شاربي

121. الأفروعربية الجديدة: أجندات جنوب أفريقيا الأفريقية
والعربية والشرق أوسطية

كريس لاندزبيرج

122. دور محكمة العدل الدولية في العالم المعاصر

القاضية روزالين هيجنز

123. من محاربين إلى سياسيين: الإسلام السلفي ومفهوم "السلام الديمقراطي"

جيمس وايلي

124. صورة العرب في الذهنية الأفريقية: حالة نيجيريا

د. الخضر عبدالباقي محمد

125. الأزمة الاقتصادية العالمية وانعكاساتها
على دول مجلس التعاون لدول الخليج العربية

د. هنري عزام

126. الصراع على السياسة والسلطة في الساحة الفلسطينية:
المقدمات والتداعيات وما العمل؟

ماجد كيالي

127. نظرة الغرب إلى الإسلام ومستقبل السلفية الإسلامية

شارل سان برو

128. الأمن الإنساني: دور القطاع الخاص في تعزيز أمن الأفراد

وولفجانج أماديوس برولهارت ومارك بروبست

129. مكافحة تمويل التهديدات عبر الحدود الوطنية

مايكل جاكوبسون وماثيو ليفيت

130. مصادر التهديد لدول الخليج العربية وسياسات الأمن لديها

د. أحمد شكارة

131. الانتخابات الرئاسية الإيرانية العاشرة وانعكاساتها الإقليمية

د. محجوب الزويري

132. العلاقات الأمريكية-الإيرانية: نحو تبني واقعية جديدة

د. محمود مونشيبوري

133. مشاركة ضرورية: إعادة تشكيل العلاقات الأمريكية مع العالم الإسلامي

د. إميل نخلة

134. المستقبل السياسي للصومال

د. عبدي عواله جامع

135. المسلمون الأمريكيون وإدارة أوباما

د. محمد نمر

136. التحديات الداخلية في باكستان وتأثيراتها في المنطقة

نعيم أحمد ساليك

137. المسلمون في أوربا بين الاندماج والتهميش

د. حسني عبيدي

138. تعزيز علاقات الشراكة بين مراكز البحوث الأمريكية والخليجية

د. جيمس ماكجان

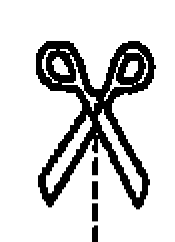
139. العراق: تداعيات ما بعد الانتخابات البرلمانية

وقرب الانسحاب الأمريكي

د. أحمد شكارة

140. حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية

ريتشارد كلارك وروبرت نيك



قسيمة اشتراك في سلسلة

«محاضرات الإمارات»

الاســم : ....

المؤسسة : ....

العنـوان : ....

ص. ب : .... المدينــة: ....

الرمز البريدي : ....

الـدولـة : ....

هـاتـف : .... فـاكـس: ....

البريد الإلكتروني: ....

بدء الاشتراك: (من العدد: .... إلى العدد: ....)

رسوم الاشتراك*

للأفـراد:	110 دراهم	30 دولاراً أمريكياً
للمؤسسات:	220 درهماً	60 دولاراً أمريكياً

- ☐ للاشتراك من داخل الدولة يقبل الدفع النقدي، والشيكات، والحوالات النقدية.
- ☐ للاشتراك من خارج الدولة تقبل فقط الحوالات المصرفية، مع تحمل المشترك تكاليف التحويل.
- ☐ في حالة الحوالة المصرفية، يرجى تحويل قيمة الاشتراك إلى حساب مركز الإمارات للدراسات والبحوث الاستراتيجية رقم 1950050565 – بنك أبوظبي الوطني – فرع الخالدية، ص. ب: 46175 أبوظبي – دولة الإمارات العربية المتحدة.
- ☐ يمكن الاشتراك عبر موقعنا على الإنترنت (www.ecssr.ae) باستعمال بطاقتي الائتمان Visa و Master Card.

لمزيد من المعلومات حول آلية الاشتراك يرجى الاتصال:

قسم التوزيع والمعارض

ص.ب: 4567 أبوظبي ـ دولة الإمارات العربية المتحدة

هاتف: 4044445 (9712) فاكس: 4044443 (9712)

البريد الإلكتروني: books@ecssr.ae

الموقع على الإنترنت: http://www.ecssr.ae

* تشمل رسوم الاشتراك الرسوم البريدية، وتغطي تكلفة اثني عشر عدداً من تاريخ بدء الاشتراك.



مركز الإمارات للدراسات والبحوث الاستراتيجية

ص.ب: 4567 ، أبوظبي ، دولة الإمارات العربية المتحدة، هاتف: 4044541-9712+ ، فاكس: 4044542-9712+
البريد الإلكتروني: pubdis@ecssr.ae ، الموقع على الإنترنت: www.ecssr.ae



ISSN 1682-122X

